IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

HARRIS CORPORATION, Plaintiff, v. HUAWEI DEVICE USA, INC., HUAWEI DEVICE CO., LTD., HUAWEI TECHNOLOGIES USA INC., HUAWEI TECHNOLOGIES CO. LTD., AND HUAWEI DEVICE (SHENZHEN) CO., LTD. Defendants.	)	CIVIL ACTION NO. 2:18-cv-439 JURY TRIAL DEMANDED

HARRIS CORPORATION'S AMENDED COMPLAINT FOR PATENT INFRINGEMENT

TO THE HONORABLE JUDGE OF SAID COURT:

Plaintiff, Harris Corporation, for its Complaint against Defendants, Huawei Device USA, Inc., Huawei Device Co., Ltd., Huawei Technologies USA Ltd., Huawei Technologies Co. Ltd., and Huawei Device (Shenzhen) Co., Ltd. (collectively "Huawei") alleges:

THE PARTIES

1. Plaintiff Harris Corporation ("Harris") is a Delaware corporation duly organized and existing under the laws of the state of Delaware with its principal place of business at 1025 West NASA Boulevard, Melbourne, Florida.

2. Defendant Huawei Device USA, Inc. ("Huawei USA") is a corporation organized under the laws of Texas with its principal place of business in this judicial district at 5700 Tennyson Parkway, Suite 300, Plano, Texas 75024.

3. Defendant Huawei Device Co., Ltd. ("Huawei China") is a Chinese company with its principal place of business in Bantian, Longgang District Shenzhen, 518129 China. Huawei China does business in Texas and in the Eastern District of Texas.

4. Defendant Huawei Technologies Co. Ltd. ("Huawei Technologies") is a Chinese corporation with its principal place of business at Huawei Industrial Base, Bantian Longgang District Shenzhen, China.

5. Defendant Huawei Technologies USA Inc. ("HTUS") is a corporation organized under the laws of Texas with its principal place of business in this judicial district at 5700 Tennyson Parkway, Suite 500, Plano, Texas, 75024.

6. Defendant Huawei Device (Shenzhen) Co., Ltd. ("HSZ") is a corporation organized and existing under the laws of the People's Republic of China with its principal place of business at Building 2, Section B, Huawei Industrial Base (Shenzhen Campus), Bantian, Longgan District, Shenzhen, Guangdong, 518129, China.

JURISDICTION

7. This is an action arising under the patent laws of the United States, 35 U.S.C. § 271, *et seq*. Accordingly, this Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

8. This Court has personal jurisdiction over Huawei due to its continuous presence in, and systematic contact with, this judicial district and Huawei USA's and HTUS's incorporation in Texas and domicile in this judicial district.

VENUE

9. Venue is proper in this judicial district pursuant to 28 U.S.C. §§1391(b), (c), (d) and 1400(b) because Huawei USA and HTUS are Texas corporations located in this judicial district. Huawei has committed, and continues to commit, acts of infringement, including providing electronic products that are used, offered for sale, sold, and have been purchased in the State of Texas, including in the Eastern District of Texas.

FACTUAL ALLEGATIONS

Harris Patents

10. Harris is an international communications and information technology company serving government and commercial markets in more than 150 countries. Harris is a proven leader in tactical communications, avionics, air traffic management, space and intelligence, and weather systems.

11. For more than 120 years, Harris has been a leader in technology and innovation. Harris currently employs more than 7,700 scientists and engineers and has advanced facilities that promote innovation and collaboration. In addition to substantial government funded research, Harris spent more than $300 million in research and development in fiscal year 2018 alone. Harris owns more than 3,000 patents that span various fields of technology.

12. United States Patent No. 6,535,227 ("the '227 Patent"), entitled "System and Method for Assessing the Security Posture of a Network and Having a Graphical User Interface," was duly and lawfully issued March 18, 2003. Harris is the owner of all right, title, and interest in the '227 Patent. A true and correct copy of the '227 Patent is attached hereto as Exhibit 1.

13. The '227 Patent describes problems and shortcomings in the field of vulnerability analysis in computer network infrastructure and claims novel and inventive technological improvements and solutions to such problems and shortcomings. By providing a data processing system and method for assessing the security vulnerability of the network, a security posture is determined efficiently. In one aspect of the invention, a graphical user interface is used for determining the vulnerability posture of a network. A system design window displays network icons of a network map that are representative of different network elements contained within a network. The respective network icons are linked together in an arrangement corresponding to how network elements are interconnected within the network. Network vulnerabilities are depicted in different colors on the network map. A graphical user interface can also comprise a manager window for displaying properties of network elements. A data sensitivity box can have user selected items for selecting the sensitivity of network elements. The graphical user interface can also comprise a select node configuration edit box having a user selectable vulnerability profile.

14. United States Patent No. 6,958,986 ("the '986 Patent"), entitled "Wireless Communication System with Enhanced Time Slot Allocation and Interference Avoidance/Mitigation Features And Related Methods," was duly and lawfully issued October 25, 2005. Harris is the owner of all right, title, and interest in the '986 Patent. A true and correct copy of the '986 Patent is attached hereto as Exhibit 2.

15. The ’986 Patent describes problems and shortcomings in the field of wireless networks and claims novel and inventive technological improvements and solutions to such problems and shortcomings. For example, Time Division Multiple Access (TDMA) is an access scheme used to establish communication links between mobile communication systems. Because an omnidirectional antenna is typically used in TDMA systems when operating at a fixed frequency, the mobile communication systems must take turns transmitting within their respective time slots to prevent channel interference. It is an object of the invention of the ’986 Patent to schedule time slots and mitigate the effects of interference in a manner that is responsive to variations in communication link demands within a mobile wireless network. For example, a controller may schedule semi-permanent time slots to establish communication links with neighboring mobile nodes for transmitting data therebetween. The controller may also determine respective link utilization metrics for each data priority level for each communication link, and schedule demand-assigned time slots for establishing additional communication links with the neighboring mobile nodes for transmitting data therebetween based upon the link utilization metrics and data priority levels.

16. United States Patent No. 6,980,537 (“the ’537 Patent”), entitled “Method and Apparatus for Communication Network Cluster Formation and Transmission of Node Link Status Messages with Reduced Protocol Overhead Traffic,” was duly and lawfully issued December 27, 2005. Harris is the owner of all right, title, and interest in the ’537 Patent. A true and correct copy of the ’537 Patent is attached hereto as Exhibit 3.

17. The ’537 Patent describes problems and shortcomings pertaining to wireless communication systems utilizing network topology information and claims novel and inventive technological improvements and solutions to such problems and shortcomings. The invention utilizes network topology information to identify network nodes crucial for relaying traffic. The

identified nodes are designated as head nodes, while remaining nodes are designated as member nodes. Since head nodes basically serve as relay nodes, the invention removes the need for gateway type nodes. In other words, the invention leverages network nodes with relay or routing capability, designating such as head nodes, to achieve connectivity among the nodes. Since the invention employs a deterministic approach, the cluster formation remains substantially the same independently of the initial start-up sequence of network nodes. Further, the designation of head nodes is optimal since the designated nodes are crucial for relaying network traffic. Moreover, since the quantity of head nodes that may facilitate communications depends upon the interval between node status packet transmissions, the invention, *inter alia*, adaptively adjusts that interval to subsequently facilitate cluster formation independent of network size and varying start times of network nodes.

18. United States Patent No. 7,017,426 ("the '426 Patent"), entitled "Multi-Channel Mobile Ad Hoc Network," was duly and lawfully issued April 11, 2006. Harris is the owner of all right, title, and interest in the '426 Patent. A true and correct copy of the '426 Patent is attached hereto as Exhibit 4.

19. The '426 Patent describes problems and shortcomings in the field of wireless networks and claims novel and inventive technological improvements and solutions to such problems and shortcomings. For example, the patent specification describes mobile ad hoc networks, in which the network does not in general depend on a particular node and dynamically adjusts as some nodes join or others leave the network. Conventional mobile ad hoc networks did not utilize multiple channels for transmitting packet data. One object of the invention is to provide a multichannel ad hoc network to make use of a plurality of channels.

20. United States Patent No. 7,224,678 ("the '678 Patent"), entitled "Wireless Local or Metropolitan Area Network with Intrusion Detection Features and Related Methods," was

duly and lawfully issued May 29, 2007. Harris is the owner of all right, title, and interest in the '678 Patent. A true and correct copy of the '678 Patent is attached hereto as Exhibit 5.

21. The '678 Patent describes problems and shortcomings in the field of wireless networks and claims novel and inventive technological improvements and solutions to such problems and shortcomings. For example, wireless local area networks (LAN) or metropolitan area networks (MAN) have significant drawbacks, including that they are readily available to would-be hackers who may attempt to intrude upon the network and compromise network security using an unauthorized wireless station. Intrusion detection software might attempt to detect intruders by monitoring packet addresses and comparing them to known addresses of authorized network stations. However, if a rogue station obtained access to an authorized address and/or ID, these approaches may not detect the intrusion of the rogue station into the networks. The '678 Patent describes novel ways of monitoring transmissions and packets to provide intrusion detection features and related methods in wireless networks. Exemplary ways of detecting intrusions include monitoring transmissions to detect frame check sequence (FCS) errors from a medium access control (MAC) address exceeding a threshold; monitoring transmissions to detect failed attempts to authenticate MAC addresses; monitoring requests-to-send and clear-to-send packets to detect illegal network allocation vector values; monitoring transmissions to detect transmissions during contention or contention-free mode; and detecting frame check sequence errors for MAC addresses exceeding a threshold.

22. United States Patent No. 7,327,690 ("the '690 Patent"), entitled "Wireless Local or Metropolitan Area Network with Intrusion Detection Features and Related Methods," was duly and lawfully issued Feb. 5, 2008. Harris is the owner of all right, title, and interest in the '690 Patent. A true and correct copy of the '690 Patent is attached hereto as Exhibit 6.

23. The ’690 Patent describes problems and shortcomings in the field of wireless networks and claims novel and inventive technological improvements and solutions to such problems and shortcomings. For example, wireless local area networks (LAN) or metropolitan area networks (MAN) have significant drawbacks, including that they are readily available to would-be hackers who may attempt to intrude upon the network and compromise network security using an unauthorized wireless station. Intrusion detection software might attempt to detect intruders by monitoring packet addresses and comparing them to known addresses of authorized network stations. However, if a rogue station obtained access to an authorized address and/or ID, these approaches may not detect the intrusion of the rogue station into the networks. The ’690 Patent describes novel ways of monitoring transmissions and packets to provide intrusion detection features and related methods in wireless networks. Exemplary ways of detecting intrusions include detecting transmissions during an unauthorized period and integrity checking for values that do not correspond with their respective data packets; detecting usage of non-consecutive MAC sequence numbers; detecting a threshold number of collisions of packets having a predetermined packet type; and detecting a threshold number of collisions of a same MAC address.

24. United States Patent No. 7,440,572 (“the ’572 Patent”), entitled “Secure Wireless LAN Device and Associated Methods,” was duly and lawfully issued October 21, 2008. Harris is the owner of all right, title, and interest in the ’572 Patent. A true and correct copy of the ’572 Patent is attached hereto as Exhibit 7.

25. The ’572 Patent describes problems and shortcomings in the field of wireless networks and claims novel and inventive technological improvements and solutions to such problems and shortcomings. For example, the ’572 Patent describes connecting computers wirelessly by means of a local area network (LAN). Security for communications can be

provided by a wireless standard, such as IEEE 802.11. To provide higher levels of security, more powerful cryptographic equipment is available, but such equipment is relatively bulky and expensive. It is an object of the invention of the '572 Patent to provide a secure wireless device, such as a LAN device, that provides greater security without significant increase in cost or complexity. For example, such devices may include a cryptography circuit that encrypts both address and data information for transmission, and decrypts both address and data information upon reception.

Huawei's Use of the Patented Technology

Huawei Intrusion Detection Products

26. On information and belief, Huawei makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States various enterprise networking equipment and solutions.

27. On information and belief, in the fall of 2011, Huawei formally launched its United States enterprise business focusing on unified communications and collaboration (UC&C), cloud computing, and enterprise information security. Huawei delivers its portfolio of products to American enterprises through channel partners including, but not limited to, WAV, TigerDirect and NewEgg. For example, on information and belief, Huawei, alone or in collaboration with its partners, recently worked or is working with a company in San Francisco, California (Cloud4Wi) to install a CloudCampus solution. https://cloud4wi.com/cloud4wi-and-huawei/.

28. Network security is a critical part of any wireless network, and it is desirable to detect attempts at network intrusion. On information and belief, Huawei's Wireless Intrusion Detection System (WIDS) and Wireless Intrusion Prevention System (WIPS) ensure network border security for Huawei networking products in small-, medium-, and large-scale enterprise

networks to help detect attacks from rogue devices. On information and belief, Huawei includes these technologies across an array of products including at least Huawei's access points, access controllers, routers, remote units and switches.

29. On information and belief, the Huawei Access Points (APs) support WIDS, WIPS and/or other similar intrusion detection and prevention technology. The Accused Huawei APs include, but are not limited to: AD9000 series, AP1000 series, AP2000 series, AP3000 series, AP4000 series, AP5000 series, AP6000 series, AP7000 series, AP8000 series, AP9000 series Access Points, the AT815SN Outdoor Access Terminal and other models that include similar functionality.

30. On information and belief Huawei remote units also support WIDS, WIPS and/or other similar intrusion detection and prevention technology. The Accused Huawei remote units include, but are not limited to: R230D, R240D, R250D, R250D-E, R251D, R251D-E, R450D Remote Units and other models that include similar functionality.

31. On information and belief, Huawei switches support WIDS, WIPS and/or other similar intrusion detection and prevention technology. The Accused Huawei switches include, but are not limited to: S12700 Series Switches, S5720-LI and S5720-SI Switches, S5700-SI Series Standard Gigabit Switches, S5700-EI Series Enhanced Gigabit Switches, S3700 Series Enterprise Switches, S6720-HI Series Agile Fixed Switches, S5730-HI Series Next generation Agile Switch and other models that include similar functionality.

32. On information and belief, Huawei Access Controllers (ACs) support WIDS, WIPS and/or other similar intrusion detection and prevention technology. The Accused Huawei ACs include, but are not limited to: AC6800V, AC6605, AC6005, ENP Series, ACU2 Wireless Access Controller Unit, and other models that include similar functionality.

33. On information and belief Huawei routers also support WIDS, WIPS and/or other similar intrusion detection and prevention technology. The routers include, but are not limited to, NE9000 Series, NE 5000E Cluster, Net Engine40E Series, NE20E Series, NE05E Series, NE08E Series, ME60 Series, AR Series, and other models that include similar functionality.

34. Huawei makes, uses, offers to sell, sells or imports into the U.S various other hardware and software that support WLAN security and intrusion detection and prevention technology, including but not limited to, Next-Generation Intrusion Prevention (NIP) devices, formerly also known as Network Intelligent Police devices, such as the NIP6000 series; Anti-DDoS devices such as the AntiDDoS1000 Series and AntiDDoS8000 Series and other hardware and software that include similar functionality. Huawei further operates and/or supports at least four Cloud Mitigation Alliance scrubbing centers in the United States (San Jose, Miami, Los Angeles and Ashburn) that work with the Anti-DDoS systems to detect and clean network traffic.

35. On information and belief, Huawei's eSight Platform, the eSight WLAN Manager and other eSight products ("Huawei eSight Products") incorporate the WIDS, WIPS and/or other similar intrusion detection and prevention technology.

Huawei Wi-Fi Products

36. On information and belief, Huawei makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States numerous WLAN products compatible with 802.11a/b/g/n/ac standards, including access points (e.g., AP1000, AP2000, AP4000, AP5000, AP6000, AP7000, AP8000, AP9000, AD9000 series of indoor and outdoor access points), access controllers (e.g., AC6000 series access controllers), routers (e.g., AR160-M series, AR161W-P-M9, and AR169RW-P-M9), access networks (e.g., DN8245W-10) and Home Wi-Fi (e.g., Q2

and A1) and other models that include similar functionality. On information and belief, at least some of these products are included in the CloudCampus Solution, discussed above.

37. Wireless Mesh Networks (WMN) consist of multiple wirelessly connected access points (nodes) that can automatically establish a wireless multi-hop network that is connected to a wired network through a portal node. Nodes in a WMN can automatically establish ad-hoc topology and maintain mesh connectivity. On information and belief, many of Huawei's WLAN products devices listed above have mesh networking capability (e.g., the Home Wi-Fi Q2 and most of the Huawei's APs and ACs listed above).

Huawei Zigbee Products

38. The Internet of Things, often referred to as IoT, is a rapidly expanding market. At a simple level, IoT is the concept of connecting any device with an on/off switch to the Internet (and/or to each other). This includes cellphones, coffee makers, washing machines, other home appliances, headphones, light fixtures, lamps, wearable fitness devices and virtually any other electrical or battery-operated device.

39. The Zigbee Alliance is the standard bearer of the open IoT. Zigbee devices are based on the IEEE 802.15.4 MAC and PHY specification.

40. The IEEE 802.15.4 standard defines the physical layer (PHY) and medium access control (MAC) sublayer specifications for low-data-rate wireless connectivity with fixed, portable, and moving devices with no battery or very limited battery consumption requirements typically operating in the personal operating space (POS) of 10 m. Zigbee is an enhancement of the IEEE 802.15.4 standard that covers the third and higher layers (including the network and application layers) of the standard model of network operation. Thus, any device that is Zigbee compliant is also compliant with the IEEE 802.15.4 standard.

41. On information and belief, the media access layer and physical layer of the IEEE 802.15.4 specifications are used at the underlying layers of Huawei's IoT solutions.

42. On information and belief, Huawei makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States, numerous Zigbee certified products. On information and belief, Huawei is a member of the Zigbee Alliance and produces products certified by Zigbee, including but not limited to the EchoLife HS2145V, LS2035V, and LS2025 smart home gateway devices, the QUIVICON Home Base and other similar products certified by Zigbee. In its product literature, Huawei identifies a number of other products as Zigbee compliant, including the AR160-M series enterprise routers (specifically the AR169RW-P-M9 router) and the X-Gen Wi-Fi AP7060DN access point.

FIRST COUNT
(Infringement of U.S. Patent No. 6,535,227)

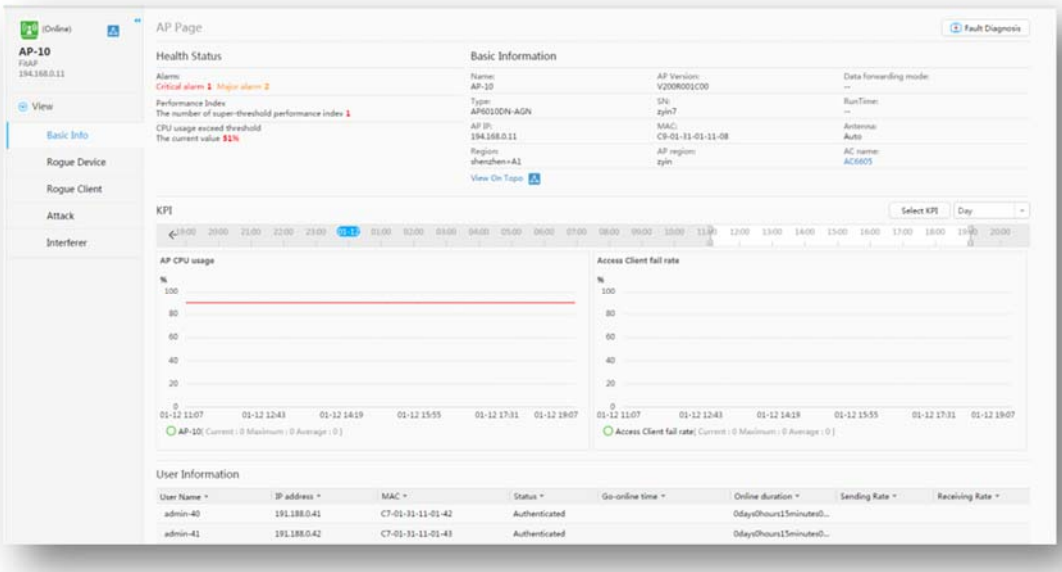
43. Harris incorporates by reference the allegations set forth in Paragraphs 1-42 of this Complaint as though fully set forth herein.

44. Huawei makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States products that directly infringe the '227 Patent, including the above identified Huawei eSight Products ('227 Accused Products). Huawei's '227 Accused Products infringe one or more claims of the '227 Patent, including without limitation, claim 24.

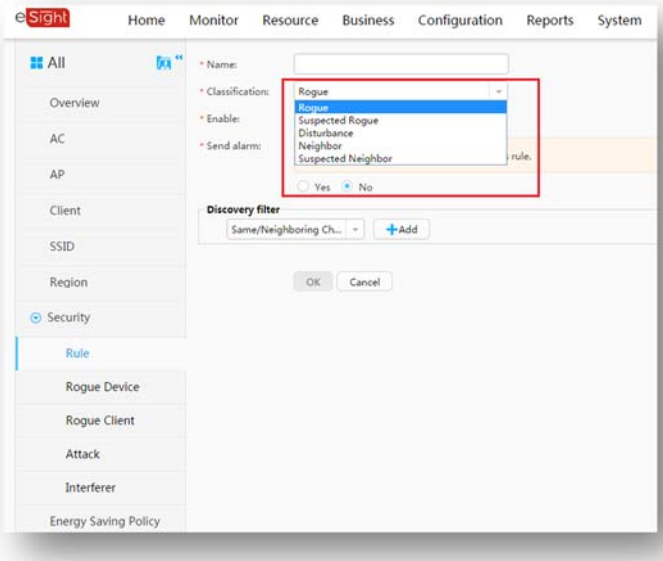
45. As an example, the '227 Accused Products contain a graphical user interface on a computer screen and used for determining the security posture of a network. The Huawei eSight Platform has a graphical user interface that displays a unified topology of devices over the entire network as well as device and link statuses in real time, simplifying topology monitoring. *See* Huawei eSight Platform, https://e.huawei.com/us/products/software/mgmt-sys/esight/esight-platform. Huawei eSight Platform displays the networking structure, device alarms, and network status over the entire network in one topology.

46. Huawei eSight has a system design window for displaying network icons of a network map that are representative of different network elements contained within a network, wherein respective network icons are linked together in an arrangement corresponding to how network elements are interconnected within the network. For example, Huawei eSight Platform has a graphical user interface that displays a unified topology of devices over the entire network as well as device and link statuses in real time, simplifying topology monitoring. *See* Huawei eSight Platform, https://e.huawei.com/us/products/software/mgmt-sys/esight/esight-platform.

47. Huawei eSight has a select node configuration edit box having a user selectable vulnerability profile for selecting a vulnerability profile of a network node. The Wireless Intrusion Detection System (WIDS) in eSight manages information about rogue devices, interference resources, and attacks, and supports type-based recognition and alarm notification based on user-defined rules. *See* Huawei eSight WLAN Technical Paper (https://e.huawei.com/ca/material/onLineView?MaterialID=90f6b3166abd445e8760fa679fac2ec6), 2017-03-20, at 10. Network administrators can classify, and filter rogue APs and management alarms based on defined rules. (*Id*. at 9.) Users can enable eSight to generate alarms when rogue APs are detected in accordance with defined rules. (*Id*.)



(*Id*. at 27.)



(*Id*. at 15.)

48. In Huawei eSight, a selected portion of the network map changes color to indicate the vulnerability that has been established for that portion of the network after a security posture of the network has been established. For example, eSight identifies alarm severity levels, such as

critical, major, minor, and warning using different colors or words. *See* Huawei eSight Platform, https://e.huawei.com/us/products/software/mgmt-sys/esight/esight-platform.

49. By making, using, offering for sale, and/or selling products in the United States, and/or importing products into the United States, including but not limited to the '227 Accused Products, Huawei has injured Harris and is liable to Harris for directly infringing one or more claims of the '227 Patent, including without limitation claim 24 pursuant to 35 U.S.C. § 271(a).

50. Huawei also infringes the '227 Patent under 35 U.S.C. § 271(b) & (c).

51. Huawei knowingly encourages and intends to induce infringement of the '227 Patent by making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the '227 Accused Products, with knowledge and specific intention that such products will be used by its customers. For example, Huawei instructs its customers on how to use and implement the technology claimed in the '227 patent. *See e.g., See* Huawei eSight Platform webpage, https://e.huawei.com/us/products/software/mgmt-sys/esight/esight-platform.

52. Huawei also contributes to the infringement of the '227 Patent. Huawei makes, uses, sells, and/or offers to sell products in the United States, and/or imports them into the United States, including but not limited to the '227 Accused Products, knowing that those products constitute a material part of the claimed invention, that they are especially made or adapted for use in infringing the '227 Patent, and that they are not staple articles or commodities of commerce capable of substantial non-infringing use.

53. On March 12, 2018, Harris informed Huawei of its infringement of the '227 Patent. Thus, as of March 12, 2018, Huawei was aware of the '227 Patent, had knowledge of the infringing nature of its activities, and nevertheless continues its infringing activities. Following

the March 12, 2018 letter, Harris attempted to contact Huawei on multiple occasions (April 25, 2018 email, May 4, 2018 email and May 25, 2018 letter), but received no response from Huawei.

54. Huawei's infringement of the '227 Patent has been and continues to be deliberate and willful, and, this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

55. As a result of Huawei's infringement of the '227 Patent, Harris has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Huawei's infringement, but in no event less than a reasonable royalty with interest and costs.

SECOND COUNT
(Infringement of U.S. Patent No. 6,958,986)

56. Harris incorporates by reference the allegations set forth in Paragraphs 1-55 of this Complaint as though fully set forth herein.

57. Huawei makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States products that comply with the Zigbee and IEEE 802.15.4 standards that directly infringe the '986 Patent, including but not limited to the Huawei Zigbee Products identified above (the '986 Accused Products). Huawei's '986 Accused Products infringe one or more claims of the '986 Patent, including without limitation claim 25 of the '986 Patent.

58. As an example, the '986 Accused Products are mobile nodes with data queues that can be assembled into a wireless communication network. For example, because the '986 Accused Products comply with IEEE 802.15.4, they contain a "coordinator" as defined and discussed in that standard, i.e., "[a] device in an [sic] low rate wireless personal area network (LR WPAN) that provides synchronization services to other devices in the LR WPAN." *See* IEEE Std. 802.15.4-2011, at § 3.1. The coordinator contains a data queue. *Id*. at § 5.1.6.4.3.

59. The '986 Accused Products schedule semi-permanent time slots to establish communication links between respective pairs of mobile nodes for transmitting data stored in the data queues therebetween. For example, because the '986 Accused Products comply with IEEE 802.15.4, they contain a MAC sublayer which feature "beacon management, channel access, GTS management, frame validation, acknowledged frame delivery, association, and disassociation." *Id*. at § 4.4.2. Further, in the MAC protocol, personal area networks (PANs) "that wish to use the superframe structure (referred to as beacon-enabled PANs) shall set macBeaconOrder to a value between 0 and 14, both inclusive, and *macSuperframeOrder* to a value between 0 and the value of *macBeaconOrder*, both inclusive." *Id*. at § 5.1.1.1

60. The '986 Accused Products determine link utilization metrics for each communication link based upon a quantity of data previously sent over the communication link during the semi-permanent time slots and the data queues. For example, because the '986 Accused Products comply with IEEE 802.15.4, they contain a Link Quality Indicator (LQI). *Id*. at § 8.2.6. Further, a "device on a beacon-enabled PAN can determine whether any frames are pending for it by examining the contents of the received beacon frame, as described in 5.1.4.1." *Id*. at § 5.1.6.3.

61. The '986 Accused Products schedule demand assigned time slots for establishing additional communication links between the pairs of mobile nodes for transmitting the data based upon the link utilization metrics. For example, because the '986 Accused Products comply with IEEE 802.15.4, they contain a superframe structure which, "[f]or low-latency applications or applications requiring specific data bandwidth, the PAN coordinator dedicates portions of the active superframe to that application." *Id*. at § 4.5.1. "GTSs shall be allocated on a first-come-first-served basis …provided there is sufficient bandwidth available." *Id*. at § 5.1.7.2

62. By making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the '986 Accused Products, Huawei has injured Harris and is liable to Harris for directly infringing one or more claims of the '986 Patent, including without limitation claim 25, pursuant to 35 U.S.C. § 271(a).

63. Huawei also infringes the '986 Patent under 35 U.S.C. § 271(b) & (c).

64. Huawei knowingly encourages and intends to induce infringement of the '986 Patent by making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the '986 Accused Products, with knowledge and specific intention that such products will be made by Huawei or by its customers into a network that infringes the '986 Patent. One example is the CloudCampus Solution being implemented for Cloud4Wi, as discussed above.

65. Huawei also contributes to the infringement of the '986 Patent. Huawei makes, uses, sells, and/or offers to sell products in the United States, and/or imports them into the United States, including but not limited to the '986 Accused Products, knowing that those products constitute a material part of the claimed invention, that they are especially made or adapted for use in infringing the '986 Patent, and that they are not staple articles or commodities of commerce capable of substantial non-infringing use.

66. On March 12, 2018, Harris informed Huawei of its infringement of the '986 Patent. Thus, as of March 12, 2018, Huawei was aware of the '986 Patent, had knowledge of the infringing nature of its activities, and nevertheless continues its infringing activities. Following the March 12, 2018 letter, Harris attempted to contact Huawei on multiple occasions (April 25, 2018 email, May 4, 2018 email and May 25, 2018 letter), but received no response from Huawei.

67. Huawei's infringement of the '986 Patent has been and continues to be deliberate and willful, and, this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

68. As a result of Huawei's infringement of the '986 Patent, Harris has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Huawei's infringement, but in no event less than a reasonable royalty with interest and costs.

THIRD COUNT
(Infringement of U.S. Patent No. 6,980,537)

69. Harris incorporates by reference the allegations set forth in Paragraphs 1-68 of this Complaint as though fully set forth herein.

70. Huawei makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States products that comply with the Zigbee and IEEE 802.15.4 standards that directly infringe the '537 Patent, including but not limited to the Huawei Zigbee Products identified above (the '537 Accused Products). Huawei's '537 Accused Products infringe one or more claims of the '537 Patent, including without limitation claim 30 of the '537 Patent.

71. Huawei communications networks are made up of two or more '537 Accused Products and comprise a plurality of communication units that transmit and receive messages within said network.

72. The '537 Accused Products comprise a status transmission module to facilitate periodic transmission of a unit status message. For example, because the '537 Accused Products comply with IEEE 802.15.4 standard, they contain a MAC sublayer that features "beacon management, channel access, GTS management, frame validation, acknowledged frame delivery, association, and disassociation." *See* IEEE Std. 802.15.4-2011 at § 4.4.2. When a '537 Accused Product, which is an IEEE 802.15.4 WPAN full-functioning device (FFD), joins the WPAN at

the PAN coordinator, it adds the PAN coordinator as its parent in its neighbor list and begins transmitting periodic beacons; other candidate devices are able to then join the network at that device. *See* IEEE Std. 802.15.4-2011 at § 4.3.2.

73. The '537 Accused Products comprise an interval module to adjust the time between each said periodic transmission in response to detecting modifications in connectivity with neighboring units. When a '537 Accused Product, which is an IEEE 802.15.4 WPAN full-functioning device (FFD), "misses between one and (*aMaxLostBeacons*–1) consecutive beacon frames from its coordinator, the device shall continue to transmit its own beacons based on both *macBeaconOrder*… and its local clock. If the device… does not lose synchronization, the device shall resume transmitting its own beacons based on the *StartTime* parameter and the incoming beacon." *See* IEEE Std. 802.15.4-2011 at § 5.1.2.4.

74. The '537 Accused Products comprise a configuration module to determine a status of that communication unit as a routing unit for routing network traffic or as a member unit of a corresponding routing unit in accordance with information contained within received unit status messages. The responsibilities of the ZDO (ZigBee Device Object) include defining the role of the device within the network (e.g., ZigBee coordinator or end device), initiating and/or responding to binding requests and establishing a secure relationship between network devices. The ZDO is also responsible for discovering devices on the network and determining which application services they provide. *See* ZigBee Specification, ZigBee Document 053474r06, Version 1.0, 2005 at 17-18.

75. In the Huawei communications network, a status of a '537 Accused Products as a said routing unit is fixed for routing subsequent network messages and re-evaluated in response to changes in network connectivity. For example, the network manager shall implement the ZigBee Coordinator, ZigBee Router or ZigBee End Device logical device types according to

configuration settings established either via a programmed application or during installation. If the device type is a ZigBee Router or ZigBee End Device, this function shall provide the ability to select an existing PAN to join and implement orphaning procedures which permit the device to re-associate with the same ZigBee Coordinator or ZigBee Router if network communication is lost. (*Id*. at 136).

76. By making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the '537 Accused Products, Huawei has injured Harris and is liable to Harris for directly infringing one or more claims of the '537 Patent, including without limitation claim 30, pursuant to 35 U.S.C. § 271(a).

77. Huawei also infringes the '537 Patent under 35 U.S.C. § 271(b) & (c).

78. Huawei knowingly encourages and intends to induce infringement of the '537 Patent by making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the '537 Accused Products, with knowledge and specific intention that such products will be made by Huawei or by its customers into a network that infringes the '537 Patent. One example is the CloudCampus Solution being implemented for Cloud4Wi, as discussed above.

79. Huawei also contributes to the infringement of the '537 Patent. Huawei makes, uses, sells, and/or offers to sell products in the United States, and/or imports them into the United States, including but not limited to the '537 Accused Products, knowing that those products constitute a material part of the claimed invention, that they are especially made or adapted for use in infringing the '537 Patent, and that they are not staple articles or commodities of commerce capable of substantial non-infringing use.

80. On March 12, 2018, Harris informed Huawei of its infringement of the '537 Patent. Thus, as of March 12, 2018, Huawei was aware of the '537 Patent, had knowledge of the

infringing nature of its activities, and nevertheless continues its infringing activities. Following the March 12, 2018 letter, Harris attempted to contact Huawei on multiple occasions (April 25, 2018 email, May 4, 2018 email and May 25, 2018 letter), but received no response from Huawei.

81. Huawei's infringement of the '537 Patent has been and continues to be deliberate and willful, and, this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

82. As a result of Huawei's infringement of the '537 Patent, Harris has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Huawei's infringement, but in no event less than a reasonable royalty with interest and costs.

FOURTH COUNT
(Infringement of U.S. Patent No. 7,017,426)

83. Harris incorporates by reference the allegations set forth in Paragraphs 1-82 of this Complaint as though fully set forth herein.

84. Huawei makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States products that use Wi-Fi and/or Zigbee radio links, including but not limited to the Huawei Zigbee Wi-Fi Products identified above (the '426 Wi-Fi Accused Products) and the Huawei Zigbee Products identified above (the '426 Zigbee Accused Products) (collectively, the '426 Accused Products) that Huawei and others combine into networks that perform the infringing process described below. The '426 Accused Products infringe one or more of the claims of the '426 Patent, including without limitation claim 8.

85. As an example, networks consisting of the '426 Accused Products perform a method for operating a mobile ad hoc network comprising a plurality of wireless mobile nodes and a plurality of wireless communication links connecting the plurality of nodes together over a plurality of electrically separate wireless channels. For example, Huawei has shown in public documentation how it uses the '426 Wi-Fi Accused Products to set up mobile ad hoc network

having a plurality of mobile nodes (e.g., mesh points or access points) connected by wireless communication links (e.g., 802.11 radio links). Huawei documentation shows Wi-Fi mesh networks connecting the nodes over more than one electrically separate wireless channel. *See, e.g.,* Huawei Configuration Guide WLAN-AC (http://support.huawei.com/enterprise/en/doc/EDOC1000141952), § 13.3, at 744 (S5720HI V200R010C00**;** Nov. 30, 2017). For the '426 Zigbee Accused Products, the 802.15.4 standard specifies a plurality of mobile nodes (e.g., Zigbee Coordinators, Zigbee Routers) connected by wireless communication links (e.g., 802.15.4 radio links) over more than one electrically separate wireless channels. *See, e.g.,* Zigbee Specification, Zigbee document 053474r06, v. 1.0, at 135 (2005).

86. Networks consisting of the '426 Accused Products perform the step of, at the source node, sending a route request over each of the plurality of electrically separate channels to discover routing to a destination node. For example, Huawei public documentation shows that the '426 Wi-Fi Accused Products support automatic route discovery. *See, e.g.,* Huawei Configuration Guide WLAN-AC at § 13.2. This discovery is done over more than one electrically separate channel. *Id*. at § 13.3. IEEE 802.15.4 documentation shows that '426 Zigbee Accused Products, which comply with the 802.15.4 standard, perform an orphan scan across a specified list of channels when they lose synchronization with the coordinator. *See, e.g.,* IEEE Std. 802.15.4-2011, at 27 (5 Sept. 2011).

87. Networks consisting of the '426 Accused Products perform the step of, at the source node, selecting a route to the destination node on at least one of the plurality of electrically separate channels. For example, for the '426 Wi-Fi Accused Products, the Huawei public documentation shows that the destination node responds to the route requests, which in turn causes the source node to select a route to the destination node on at least one of the

channels. *See, e.g.,* Huawei Configuration Guide WLAN-AC at § 13.2. For the '426 Zigbee Accused Products, the standard documentation shows that the Zigbee coordinator returns a coordinator realignment command to the source node, which causes it to select a route to the destination node on at least one of the channels. *See, e.g.,* IEEE Std. 802.15.4-2011, at 27.

88. By making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the '426 Accused Products, Huawei has injured Harris and is liable to Harris for directly infringing one or more claims of the '426 Patent, including without limitation claim 8, pursuant to 35 U.S.C. § 271(a).

89. Huawei also infringes the '426 Patent under 35 U.S.C. § 271(b) & (c).

90. Huawei knowingly encourages and intends to induce infringement of the '426 Patent by making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the '426 Accused Products, with knowledge and specific intention that such products will be made by Huawei or by its customers into a network that infringes the '426 Patent, as shown by Huawei documentation for customers, such as Huawei Configuration Guide WLAN-AC referenced above.

91. Huawei also contributes to the infringement of the '426 Patent. Huawei makes, uses, sells, and/or offers to sell products in the United States, and/or imports them into the United States, including but not limited to the '426 Accused Products, knowing that those products constitute a material part of the claimed invention, that they are especially made or adapted for use in infringing the '426 Patent, and that they are not staple articles or commodities of commerce capable of substantial non-infringing use.

92. On March 12, 2018, Harris informed Huawei of its infringement of the '426 Patent. Thus, as of March 12, 2018, Huawei was aware of the '426 Patent, had knowledge of the infringing nature of its activities, and nevertheless continues its infringing activities. Following

the March 12, 2018 letter, Harris attempted to contact Huawei on multiple occasions (April 25, 2018 email, May 4, 2018 email and May 25, 2018 letter), but received no response from Huawei.

93. Huawei's infringement of the '426 Patent has been and continues to be deliberate and willful, and, this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

94. As a result of Huawei's infringement of the '426 Patent, Harris has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Huawei's infringement, but in no event less than a reasonable royalty with interest and costs.

FIFTH COUNT
(Infringement of U.S. Patent No. 7,224,678)

95. Harris incorporates by reference the allegations set forth in Paragraphs 1-94 of this Complaint as though fully set forth herein.

96. Huawei makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States products that directly infringe the '678 Patent, including but not limited to the above identified Huawei Intrusion Detection Products that support WIDS, WIPS and/or other similar intrusion detection and prevention technology ('678 Accused Products). Huawei's '678 Accused Products infringe one or more claims of the '678 Patent, including without limitation, claim 12 of the '678 Patent.

97. Huawei Wireless LANs/MANs are made up of two or more '678 Accused Products and comprise a plurality of stations for transmitting data therebetween using a MAC layer, each of said stations having a respective MAC address associated therewith. For example, Huawei '678 Accused Products, transmit data therebetween. On information and belief, the '678 Accused Products comply with one or more of the IEEE 802.11 standards and transmit data using MAC layers and further have a MAC address associated therewith.

98. Huawei Wireless LAN/MAN contain a policing station for detecting intrusions into the wireless network by monitoring transmissions among said plurality of stations to detect failed attempts to authenticate MAC addresses. For example, Huawei eSight and WLAN devices that incorporate the WIDS, WIPS and/or intrusion alert technology, including at least APs and ACs, are capable of detecting flood attacks, spoofing attacks, weak initialization vector (IV) attacks, and can also defend the WLAN against brute force cracking. *See generally* Huawei's WLAN WIDS & WIPS Technology White Paper (https://e.huawei.com/us/material/onLineView?materialid=b81ebd45523d4d6591d00aa98b99692c), 2017-07-05. Brute force cracking attacks also exist when a user authentication mode is used, such as MAC address. (*Id*. at 15.) The WIDS and intrusion detection systems thus detect failed attempts to authenticate MAC addresses.

99. The Huawei Wireless LANs/MANs generate an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address. For example, when an attack is detected, the AP may report an intrusion alert to the AC. (*Id*. at 15-16.) Further, when an AC identifies an AP as a rogue AP, a rogue AP alarm is triggered and sent to the network management system (NMS). (*Id*.)

100. By making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the '678 Accused Products, Huawei has injured Harris and is liable to Harris for directly infringing one or more claims of the '678 Patent, including without limitation claim 12, pursuant to 35 U.S.C. § 271(a).

101. Huawei also infringes the '678 Patent under 35 U.S.C. § 271(b) & (c).

102. Huawei knowingly encourages and intends to induce infringement of the '678 Patent by making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the '678 Accused Products,

with knowledge and specific intention that such products will be used by its customers. One example is Huawei's supporting documentation instructing customers how to implement the technology claimed in the '678 patent. *See e.g.,* Huawei's WLAN WIDS & WIPS Technology White Paper (https://e.huawei.com/us/material/onLineView?materialid=b81ebd45523d4d6591d00aa98b99692c), 2017-07-05.

103. Huawei also contributes to the infringement of the '678 Patent. Huawei makes, uses, sells, and/or offers to sell products in the United States, and/or imports them into the United States, including but not limited to the '678 Accused Products, knowing that those products constitute a material part of the claimed invention, that they are especially made or adapted for use in infringing the '678 Patent, and that they are not staple articles or commodities of commerce capable of substantial non-infringing use.

104. On March 12, 2018, Harris informed Huawei of its infringement of the '678 Patent. Thus, as of March 12, 2018, Huawei was aware of the '678 Patent, had knowledge of the infringing nature of its activities, and nevertheless continues its infringing activities. Following the March 12, 2018 letter, Harris attempted to contact Huawei on multiple occasions (April 25, 2018 email, May 4, 2018 email and May 25, 2018 letter), but received no response from Huawei.

105. Huawei's infringement of the '678 Patent has been and continues to be deliberate and willful, and, this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

106. As a result of Huawei's infringement of the '678 Patent, Harris has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Huawei's infringement, but in no event less than a reasonable royalty with interest and costs.

SIXTH COUNT
(Infringement of U.S. Patent No. 7,327,690)

107. Harris incorporates by reference the allegations set forth in Paragraphs 1-106 of this Complaint as though fully set forth herein.

108. Huawei makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States products that directly infringe the '690 Patent, including but not limited to the above identified Huawei Intrusion Detection Products that support WIDS, WIPS and/or other similar intrusion detection and prevention technology ('690 Accused Products). Huawei's '690 Accused Products infringe one or more claims of the '690 Patent, including without limitation, claim 40 of the '690 Patent.

109. Huawei wireless LAN/MAN are made up of two or more '690 Accused Products and comprises a plurality of stations for transmitting data via a MAC layer, each station having a MAC address associated therewith to be transmitted with data sent therefrom. For example, Huawei '690 Accused Products transmit data therebetween. On information and belief, all Huawei Access Points and the '690 Accused Products comply with one or more of the IEEE 802.11 standards and transmit data using MAC layers and further have a MAC address associated therewith to be transmitted with data sent therefrom.

110. Huawei Wireless LAN/MAN contain a policing station for detecting intrusions into the wireless network by monitoring transmissions among said plurality of stations to detect collisions of a same MAC address. For example, Huawei eSight and WLAN devices that incorporate the WIDS and/or intrusion alert technology, including at least APs, ACs, are capable of detecting flood attacks, spoofing attacks, weak initialization vector (IV) attacks, and can also defend the WLAN against brute force cracking. *See generally* Huawei's WLAN WIDS & WIPS Technology White Paper (https://e.huawei.com/us/material/onLineView?materialid=b81ebd45523d4d6591d00aa98b9969

2c), 2017-07-05. A flood attack occurs when an AP receives a large number of management packets or null packets of the same type from a source MAC address within a short period. (*Id*. at 12.) WIDS can detect 802.11 packet flood, and attack information reported by an AP that includes the rogue device MAC address. (*Id*.)

111. The Huawei Wireless LAN/MAN networks generate an intrusion alert based upon detecting a threshold number of collisions of a same MAC address. For example, in the '690 Accused Products using WIDS, when the traffic received from a device exceeds the allowed threshold, the AP considers that the device is initiating a flood attack and reports an alarm message to the AC. (*Id*. at 17.) Further, when an AC identifies an AP as a rogue AP, a rogue AP alarm is triggered and sent to the network management system (NMS). (*Id*.)

112. By making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the '690 Accused Products, Huawei has injured Harris and is liable to Harris for directly infringing one or more claims of the '690 Patent, including without limitation claim 40, pursuant to 35 U.S.C. § 271(a).

113. Huawei also infringes the '690 Patent under 35 U.S.C. § 271(b) & (c).

114. Huawei knowingly encourages and intends to induce infringement of the '690 Patent by making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the '690 Accused Products, with knowledge and specific intention that such products will be used by its customers. One example is Huawei's supporting documentation instructing customers how to implement the technology claimed in the '690 patent. *See e.g.,* Huawei's WLAN WIDS & WIPS Technology White Paper (https://e.huawei.com/us/material/onLineView?materialid=b81ebd45523d4d6591d00aa98b99692c), 2017-07-05.

115. Huawei also contributes to the infringement of the '690 Patent. Huawei makes, uses, sells, and/or offers to sell products in the United States, and/or imports them into the United States, including but not limited to the '690 Accused Products, knowing that those products constitute a material part of the claimed invention, that they are especially made or adapted for use in infringing the '690 Patent, and that they are not staple articles or commodities of commerce capable of substantial non-infringing use.

116. On March 12, 2018, Harris informed Huawei of its infringement of the '690 Patent. Thus, as of March 12, 2018, Huawei was aware of the '690 Patent, had knowledge of the infringing nature of its activities, and nevertheless continues its infringing activities. Following the March 12, 2018 letter, Harris attempted to contact Huawei on multiple occasions (April 25, 2018 email, May 4, 2018 email and May 25, 2018 letter), but received no response from Huawei.

117. Huawei's infringement of the '690 Patent has been and continues to be deliberate and willful, and, this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

118. As a result of Huawei's infringement of the '690 Patent, Harris has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Huawei's infringement, but in no event less than a reasonable royalty with interest and costs.

SEVENTH COUNT
(Infringement of U.S. Patent No. 7,440,572)

119. Harris incorporates by reference the allegations set forth in Paragraphs 1-118 of this Complaint as though fully set forth herein.

120. Huawei makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States products that comply with the Zigbee and IEEE 802.15.4 standards that directly infringe the '572 Patent, including but not limited to the Huawei Zigbee Products identified above (the '572 Accused Products). Huawei's '572 Accused Products

infringe one or more claims of the '572 Patent, including without limitation claim 1 of the '572 Patent.

121. As an example, Huawei makes, uses, sells, and/or offers for sale in the United States, and imports into the United States secure wireless LAN devices. For example, because the '572 Accused Products comply with IEEE 802.15.4, they comprise a "device" as defined and discussed in that standard, i.e., "[a] system conforming to this standard consists of several components. The most basic is the device. Two or more devices communicating on the same physical channel constitute a WPAN." *See* IEEE Std 802.15.4-2011, at § 4.2. These devices are secure. *Id*. at Ch. 7 (Security).

122. The '572 Accused Products comprise a housing in which the electronic components of the device are contained.

123. The '572 Accused Products comprise a wireless transceiver carried by said housing. For example, because the '572 Accused Products comply with IEEE 802.15.4, their housings contain a wireless transceiver. *Id*. at § 4.2. ("An LR-WPAN [low-rate wireless personal area network] is a simple, low-cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements.")

124. The '572 Accused Products comprise a MAC carried by said housing for implementing a predetermined wireless LAN MAC protocol. For example, because the '572 Accused Products comply with IEEE 902.15.4 standard, they use the LAN MAC protocol specified in detail in chapter 5 of the standard.

125. The '572 Accused Products comprise a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver for encrypting both address and data information for transmission by at least adding a plurality of encrypting bits to both the address and data information, and for decrypting both the address and the data information upon

reception. For example, because the '572 Accused Products comply with IEEE 902.15.4 standard, they follow a specific security protocol as set forth in chapter 7 of the standard, which specifies inputs to the CCM* encryption transformation including a nonce (which contains address information), an encryption key, and data. *See, e.g., id.* at §§ 7.3.2 & 7.3.4.

126. By making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the '572 Accused Products, Huawei has injured Harris and is liable to Harris for directly infringing one or more claims of the '572 Patent, including without limitation claim 1 pursuant to 35 U.S.C. § 271(a).

127. Huawei also infringes the '572 Patent under 35 U.S.C. § 271(b) & (c).

128. Huawei knowingly encourages and intends to induce infringement of the '572 Patent by making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the '572 Accused Products. One example is the CloudCampus Solution being implemented for Cloud4Wi, as discussed above.

129. Huawei also contributes to the infringement of the '572 Patent. Huawei makes, uses, sells, and/or offers to sell products in the United States, and/or imports them into the United States, including but not limited to the '572 Accused Products, knowing that those products constitute a material part of the claimed invention, that they are especially made or adapted for use in infringing the '572 Patent, and that they are not staple articles or commodities of commerce capable of substantial non-infringing use.

130. On March 12, 2018, Harris informed Huawei of its infringement of the '572 Patent. Thus, as of March 12, 2018, Huawei was aware of the '572 Patent, had knowledge of the infringing nature of its activities, and nevertheless continues its infringing activities. Following

the March 12, 2018 letter, Harris attempted to contact Huawei on multiple occasions (April 25, 2018 email, May 4, 2018 email and May 25, 2018 letter), but received no response from Huawei.

131. Huawei's infringement of the '572 Patent has been and continues to be deliberate and willful, and, this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

132. As a result of Huawei's infringement of the '572 Patent, Harris has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Huawei's infringement, but in no event less than a reasonable royalty with interest and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment and seeks relief against Huawei as follows:

(a) For judgment that U.S. Patent Nos. 6,535,227; 6,980,537; 6,958,986; 7,027,426; 7,224,678; 7,327,690; and 7,440,572 have been and continue to be infringed by Huawei;

(b) For an accounting of all damages sustained by Plaintiff as the result of Huawei's acts of infringement;

(c) For finding that Huawei's infringement is willful and enhancing damages pursuant to 35 U.S.C. § 284;

(d) For a mandatory future royalty payable on each and every future sale by Huawei of a product that is found to infringe one or more of the Patents-in-Suit and on all future products which are not colorably different from products found to infringe;

(e) For an award of attorneys' fees pursuant to 35 U.S.C. § 285 or otherwise permitted by law;

(f) For all costs of suit; and

(g) For such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure and Local Rule CV-38, Plaintiff demands a trial by jury of this action.

Dated: February 15, 2019

Respectfully Submitted,

By: /s/ *Denise De Mory*

Henry C. Bunsow
Denise De Mory
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: (650) 351-7248
Facsimile: (415) 426-4744
hbunsow@bdiplaw.com
ddemory@bdiplaw.com

ATTORNEYS FOR PLAINTIFF
HARRIS CORPORATION